UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/504,150	02/15/2000	Michael George Bunn	190-1445	7518

23644 7590 11/24/2004

BARNES & THORNBURG
P.O. BOX 2786
CHICAGO, IL 60690-2786

EXAMINER	
KIM, JUNG W	
ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 11/24/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/504,150	BUNN, MICHAEL GEORGE	
	Examiner	Art Unit	
	Jung W Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 August 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *3,4,6-11 and 16-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) *17-20* is/are allowed.

6)☒ Claim(s) *6-11 and 16* is/are rejected.

7)☐ Claim(s) *3 and 4* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 February 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 3, 4, 6-11 and 16-20 have been examined. Applicant in the amendment filed on August 9, 2004, amended claims 3, 4 and 16, added new claims 17-20 and canceled claims 2 and 5. Claims 1 and 12-15 were canceled in a previous amendment.

Response to Arguments

2. The following is a response to Applicant's arguments on pages 6-8 of the amendment filed on August 9, 2004.

3. Applicant's argument with respect to the 35 U.S.C. 112, second paragraph rejection of claim 16 that a printout of the test certificate is not an essential step of the claimed invention has been fully considered and is persuasive. The aforementioned 112, second paragraph rejection of claim 16 has been withdrawn.

4. In regards to Applicant's argument, page 7, 3rd full paragraph, that there would be no reason for one skilled in the art to contemplate using a third-party arbitrator to certify the output from the device contained within a secure perimeter, examiner points to the following excerpt in Walker: see col. 3, lines 56-58.

5. In regards to Applicant's argument, page 7, 4th full paragraph, that there is no suggestion in the prior art of record that digital techniques might be used for paper

documents and hence there is no clear suggestion to a person skilled in the art using a digital signature from a third party arbitrator to certify Walker's paper printout, examiner disagrees. Walker clearly identifies means for implementing cryptographic digital techniques within physical documents, wherein one physical document is a paper document. See Walker, col. 2, line 62-col. 3, line 50; col. 5, lines 11-22; col. 11, lines 8-12.

6. In regards to Applicant's argument, page 7, last paragraph-page 8, 1st paragraph, that the digital signatures taught by Schneier "certify that a document originated from a particular person and has not been altered, but they do not check that the person was authorized to produce that document" (see Remarks, page 7, last paragraph, second sentence), examiner disagrees. Since digital signatures using symmetric cryptosystems require shared secret keys and only participants having access to these keys is privy to checking the validity of the signature, the limitation of checking whether a person was authorized to produce a document is within the scope of certifying that a document originated from a particular person using a symmetric key cryptosystem.

7. Finally, in view of the amendments to claims 3 and 4, specifically that the test certificate is printed on a blank test certificate which includes a pre-printed serial number wherein the test certificate producer sends the pre-printed serial number to the authentication authority, which makes the term "pre-printed serial number" definite, the

prior art rejections to these claims are withdrawn, and hence applicant's argument on this matter is moot.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 2-4, 6-11, and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Walker et al. U.S. Patent No. 5,828,751 (hereinafter Walker) in view of Schneier Applied Cryptography 2nd Edition (hereinafter Schneier). As per claim 16, Walker discloses a method for producing and authenticating a printed test certificate comprising the following steps:

a. a test certificate producer performs a test and cryptographically generates an authentication code from the information (see Walker, col. 3, lines 53-67; col. 4, lines 25-42);

b. the test certificate producer prints the test certificate when the authentication code is prepared, including both the information and the authentication code (see Walker, col. 4, lines 25-30; col. 16, lines 25-57, especially lines 33-36); and

c. upon presentation of the printed test certificate for authentication, a certificate checker cryptographically checks the authentication code against the

information in the printed test certificate to determine whether the printed test certificate is authentic (see Walker, col. 11, lines 8-12; col. 16, lines 25-57).

10. Walker does not specify an authentication authority receiving information from the test certificate producer, verifying that the test certificate producer is allowed to take the test and if so, cryptographically generating an authentication code from the information, then sending the authentication code to the test certificate producer. However, these limitations are found in systems that incorporate a trusted arbitrator to perform the certification. Schneier teaches such an example wherein a first party transmits a message to a trusted arbitrator, the trusted arbitrator verifies the identity of the sender of the message, certifies the message, and transmits the signed message to a second party (see Schneier, page 35-36, 'Signing Documents with Symmetric Cryptosystems and an Arbitrator'). Furthermore, Schneier teaches the use of digital signatures based on public-key cryptography and hashes of a message as a means for an arbiter to certify a message (see Schneier, page 186, 'certification authority', first paragraph; pages 38-39, 'Signing Documents with Public-Key Cryptography and One-Way Hash Functions'; page 35, 4th characteristic of a digital signature). It would be obvious to one of ordinary skill in the art at the time the invention was made to apply the teaching of Schneier to the method of Walker. Motivation for such a combination enables the method to centralize sensitive operations in a trusted party as taught by Schneier. Finally, in the case where the first and second parties are the same in the teaching of Schneier, the method covered by Walker in view of Schneier covers the applicant's claim. The aforementioned covers claim 16.

11. As per claim 6, Walker covers a method as outlined above in the claim 16 rejection under 35 U.S.C. 103(a). In addition, the certificate checker performs the following steps:

a. entering the authentication code into a computer (see Walker, col. 11, lines 11-12; col. 16, lines 46-57);

b. entering information in the printed certificate into the computer (see Walker, col. 11, lines 8-9);

c. causing the computer to cryptographically generate a check code from the information (see Walker, col. 11, lines 10-11); and

d. causing the computer to compare the check code with the authentication code (see Walker, col. 11, lines 11-12).

12. Finally, inherent in a comparison test to check the validity of an authentication code is a generated message to indicate the success or failure of the validity check. The aforementioned covers claim 6.

13. As per claim 7, Walker covers a method as outlined above in the claim 16 rejection under 35 U.S.C. 103(a). In addition, the authentication authority cryptographically generates the authentication code using a cryptographic key associated with the authentication authority (see Walker, col. 4, lines 25-42; col. 5, lines 49-65; see Schneier, page 35, 'Signing Documents with Symmetric Cryptosystems and an Arbitrator', page 36, 1st characteristic).

14. As per claim 8, Walker covers a method as outlined above in the claim 7 rejection under 35 U.S.C. 103(a). In addition, in an arbitrated method, a certification using a one-way hash necessarily uses a secret cryptographic key that is known by the authentication authority and the certificate checker, and not the producer. The producer must not know the secret cryptographic key, otherwise the producer would be able to generate hashes without the knowledge of the trusted arbiter and consequently defeat the purpose of an arbitrated certification methodology.

15. As per claim 9, Walker covers a method as outlined above in the claim 8 rejection under 35 U.S.C. 103(a). In addition, the authentication code is generated by performing a key-dependent one-way hash of the information, using the secret key (see Walker, col. 4, lines 25-29; col. 5, lines 49-57).

16. As per claim 10, Walker covers a method as outlined above in the claim 7 rejection under 35 U.S.C. 103(a). In addition, the authentication authority generates the authentication code using the private key of a public/private key pair, and wherein the certificate checker checks the authentication code using the public key of the public/private key pair (see Walker, col. 5, lines 57-62).

17. As per claim 11, Walker covers a method as outlined above in the claim 16 rejection under 35 U.S.C. 103(a). In addition, the communication between the test

certificate producer and the authentication authority is protected by encryption (see Schneier, page 35, 'Signing Documents with Symmetric Cryptosystems and an Arbitrator', steps 1, 2, 4, and 5).

Allowable Subject Matter

18. Claims 17-20 are allowable.

19. Claims 3 and 4 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

20. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (571) 272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132

Jk
November 19, 2004

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100